(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/015011 A1

(51) International Patent Classification[7]: G06K 9/00

(21) International Application Number: PCT/KR02/01251

(22) International Filing Date: 2 July 2002 (02.07.2002)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
2001/47576 7 August 2001 (07.08.2001) KR

(71) Applicant and
(72) Inventor: **KOO, Hong-Sik** [KR/KR]; 101, Heejung Mansion, 18-24, Yeokchon-dong, Eunpyung-ku, 122-070 Seoul (KR).

(74) Agent: **KIM, Samsoo**; 3rd floor, Dukwon Bldg., 637-19, Yoksam dong, Kangnam-ku, 135-909 Seoul (KR).

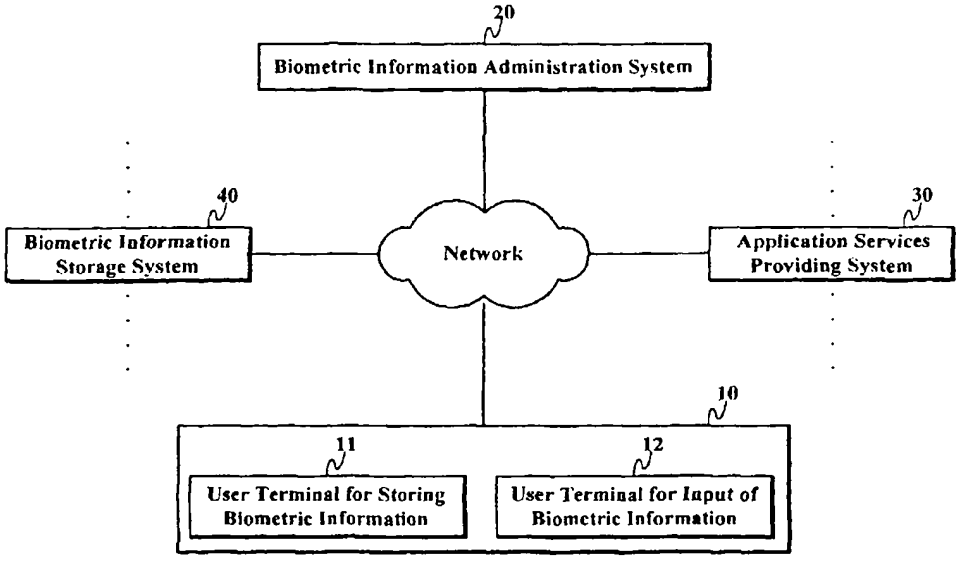
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AUTHENTICATION METHOD USING BIOMETRIC INFORMATION



(57) Abstract: Biometric information is divided into a plurality of groups and stored separately. They are transmitted to an authentication device and reconstructed to the original which is then used for authentication. Alternatively, partial authenfications are performed by a plurality of authentication devices using each group. Final authentication is done based on the results of the partial authentications. Separate storages for the divided information may be connected each other by a communication network. Examples of the biometric information are a fingerprint, an iris, and a voice pattern.

WO 03/015011 A1

AUTHENTICATION METHOD USING BIOMETRIC INFORMATION

Technical Field of the Invention

The present invention relates to a method for authentication using biometric information, and, in particular, to a method for authentication, wherein biometric information is divided into a plurality of groups and stored separately; which are collected in an authentication device where they are reconstructed to the original biometric information for authentication; or which are used individually for partial authentications performed by a plurality of authentication devices, so that a final authentication is done based on these partial authentications.

Background of the Invention

As the Internet is used widely, users are allowed to access a large variety of sites to be provided with services they desire. However, for certain services provided on the Internet obtaining a membership is obligatory, for which procedure registration of data such as membership ID, password, resident's registration number (personal ID number), etc. are required for identification of the users. And a user undergoes an authentication process by inputting his membership ID, password, etc. to be provided with such services.

Further, an authentication procedure is not only requested for use of certain online services, but also for various offline lock devices. For example, there are systems, which can store user information such as a password and allows only those users who have inputted the correct password and passed the authentication process to access the system.

Along with the development of relevant sciences and technologies, devices utilizing biometric information (fingerprint information, iris information, voice pattern

information, etc.) of users for the purpose of user authentication have recently been developed to find increasing adoption, inter alia, in various lock devices. Moreover, with widespread use of computer and its accessories such as mouse, key board, etc., devices capable of inputting and/or recognizing biometric information in a computer or the above accessory devices have also been traded increasingly, and as a result, user authentication methods utilizing biometric information are spreading in online electronic commerce and home banking as well.

However, since various user information, biometric information, authentication certificates required for the above-described user authentication are stored and administered in PCs, smart cards, USB keys, RF card keys, various lock devices, or in the server of respective electronic commerce systems, they are liable to cause huge damages for the users once such storage means are stolen or the above lock devices or the above server is hacked by an external intruder, resulting in leakage of the user information.

Here, in case authentication information consisting only of user ID or password, and the like has been leaked, the damage can remain relatively limited, while a leakage of biometric information used for an authentication process in the above lock devices or electronic commerce can cause a far greater damage in view of its wider scope of applications. In other words, in case a fingerprint information has been leaked, all lock devices and electronic commerce systems using that fingerprint information remain vulnerable, so that an unauthorized user utilizing such leaked fingerprint information is authenticated to be an authorized user. As a result, a user with extended usage of his biometric information may risk higher damages.

Detailed Description of the Invention

The present invention, conceived in view of the above problems, aims to provide a method for authentication in systems utilizing various biometric information, by dividing biometric information into a plurality of groups and storing the same in separate storage means for use in authentication of a user, while preventing leakage of the biometric information and ensuring security of the system.

According to this method, biometric information of a user to be registered is divided into a predetermined number of groups after it has been inputted from a biometric information input device, to be subsequently stored separately in a plurality of storage means, and then registered.

An authentication process utilizing the biometric information proceeds as follows: Biometric information of a user as inputted through the biometric information input device is divided into groups in the same manner and number as at the time of registration, and compared with the divided biometric information stored separately in the plural storage means, and a user is authenticated to be an authorized user only when all of the divided biometric information inputted coincide with their corresponding divided biometric information stored.

Alternatively, relevant divided biometric information stored scattered in a plurality of storage means can be connected to one another to be reconstructed to the original biometric information, upon input of the biometric information of a user from a biometric information input device, and then, the reconstructed biometric information can be compared with the biometric information of the user to be authenticated, to enable authentication of that user as an authorized user if the user's biometric information coincides with the reconstructed biometric information.

The above plural storage means can be connected to an authentication device via a

communication network. In addition, the above biometric information input device can be connected by wire or wireless to an authentication device.

Biometric information means here user information utilizing the peculiar physical information of a user, such as fingerprint pattern, voice pattern, iris pattern, etc.

Division of biometric information such as a fingerprint can be performed in various manners, e.g. dividing a fingerprint image into several sections and then extracting the fingerprint minutiae of each divided image, dividing the fingerprint minutiae as extracted from the undivided fingerprint by characteristic features, dividing the extracted fingerprint information bits using a predetermined rule, etc.

Brief Description of the Drawings

Fig. 1a shows the construction of an embodiment example of the system for divisional storage of biometric information and for authentication, to which the present invention applies.

Figs. 1b and 1c are flow charts for an embodiment example of the authentication method using biometric information in accordance with the present invention.

Fig. 2a shows the construction of another embodiment example of the system for divisional storage of biometric information and for authentication, to which the present invention applies.

Figs. 2b and 2c are flow charts for another embodiment example of the authentication method using biometric information in accordance with the present invention.

Fig. 2d shows the construction of an embodiment example of the database to which the present invention applies.

Description of the Preferred Embodiments

The preferred embodiments of the present invention are described below in detail, making reference to the appended drawings.

Fig. 1a, being a construction of an embodiment example of the authentication system using biometric information to which the present invention applies, shows a door lock system using biometric information. Further, Figs. 1b and 1c, being flow charts for an embodiment example of the authentication method using biometric information in accordance with the present invention, shows an authentication method using biometric information in the biometric authentication system in Fig. 1a.

In this embodiment, the biometric information required for locking/unlocking a door, e.g. fingerprint information, voice information, iris information, and the like is stored as divided in a plurality of storage means so that either the separately stored biometric information is collected to be reconstructed to the original biometric information for an authentication process of a user, or an authentication is performed for each divided and separately stored partial biometric information, to enable locking/unlocking of the door.

For the convenience of explanation, the process of dividing and separate storing of the divided biometric information is described below in the example of fingerprint information among divergent biometric information. For instance, a user can store his fingerprint information as divided in two storage means, i.e. in a biometric information administration system 60 (hereinafter, to be simplified as "lock device") and in a user terminal 50 (hereinafter, to be simplified as "electronic key"). Such lock device and electronic key can have a construction similar to those disclosed e.g. in PCT/KR01/01318 or PCT/KR01/02167.

When a user inputs his fingerprint information using an electronic key to open a door, the fingerprint information inputted by the user is compared with the corresponding fingerprint information generated by combination of the divided and separately stored fingerprint information, to enable a determination as to whether or not to open the door. Alternatively, an authentication can be performed in respect to each divided fingerprint information after the fingerprint information inputted by the user has been divided in groups, and then, compared with the corresponding divided fingerprint information stored separately.

The electronic key can be connected to the lock device via a wired or wireless network, via infrared communication such as IrDA, via radio communication such as blue tooth, or via wired communication such as RS-232C. Moreover, the lock device can be connected to a plurality of lock devices through a communication network as well.

Next, the processes of divisional registration of a fingerprint using an electronic key in the above system and of locking/unlocking a door are explained below.

First, a user stores his fingerprint information in an electronic key 50 or in a lock device 60 by inputting the same via the electronic key 50 or the lock device 60 (102). It is also possible that the first registration of a fingerprint is allowed only to a key administrator. Further, it is possible that the fingerprints of a plurality of users are registered in one electronic key.

Upon input of a user's fingerprint information into an electronic key 50, the electronic key 50 divides the inputted user fingerprint information into two, stores one half of the divided fingerprint information in the storage means of its own and transmits the other half to the lock device 60. The lock device 60 stores the fingerprint information thus received in its storage means (104).

On the other hand, fingerprint information can also be registered via a lock device 60. In such a case, the lock device 60 divides the inputted fingerprint information into two, stores one half of the divided fingerprint information in the storage means of its own and transmits the other half to the electronic key 50 so that it is stored in the storage means of the electronic key 50.

In case an electronic key is used by a plurality of users, it is preferable that user information such as user ID is inputted as well for identification of the user, in which case the user information is transmitted together with the divided fingerprint information to the corresponding device.

If a user, who has stored his fingerprint information as divided in both the electronic key 50 and the lock device 60 through the above procedure, wishes to lock/unlock a door using the electronic key 50, he has to input his fingerprint information in the electronic key 50 (106).

In case the electronic key is used by a plurality of users, an additional process of selecting one user among the registered users may be adopted for identification of the user.

Upon input of fingerprint information of a user to be authenticated, the electronic key 50 compares the inputted user fingerprint information with the corresponding fingerprint information stored in the storage means in the electronic key 50 (108). That is, the divided fingerprint information stored in the electronic key 50 is compared selectively with the corresponding part of the inputted fingerprint information (the part of the fingerprint information identical with that stored in the electronic key).

If any coinciding part is existent, an authentication confirm signal, the other part of the divided fingerprint information of the user, and the user information are transmitted to the lock device 60. The user information can be determined either by selecting one user

among the registered users, or by the user information of a user having a coinciding fingerprint among the plural fingerprint information stored in the storage means at the above step 108.

The lock device 60 compares the transmitted fingerprint information of a user to be authenticated with the divided fingerprint information stored in the lock device 60 (110). If the electronic key is used by a plurality of users, the fingerprint information of a user to be authenticated is compared with the fingerprint information of the user corresponding to the user information received.

If the comparison yields any coinciding part (of the fingerprint information), the fingerprint information (inputted) is recognized to be that of an authorized user, and the door is locked/unlocked (112).

Alternatively, the inputted fingerprint information as well as the divided fingerprint information stored in the storage means of the electronic key 50 can be directly transmitted to the lock device 60 without the above comparison procedure (108) as shown in Fig. 1c (158).

Here, the lock device 60 compares the divided fingerprint information transmitted from the electronic key 50 after having combined the same with the divided fingerprint information stored in the storage means of the lock device 60, or each of the uncombined fingerprint information stored in the storage means of the lock device with the fingerprint information inputted by the electronic key 50 (160), and recognizes the inputted fingerprint information as that of an authorized user if two fingerprint information coincide, to subsequently effect a locking/unlocking of the door (162).

On the other hand, in case each electronic key is determined for a certain user, it is preferable that the electronic key 50 transmits information on the electronic key itself

together with the user's fingerprint information to the lock device.

A door in the above description comprises not only a door in a building, but also all lock devices including a vehicle door. In addition, the above fingerprint information can also be stored divided in other storage means a user chooses, not restricted to the above two means, the electronic key 50 and the lock device 60, in which case information on such other storage means can be administered by the lock device in a separate database.

Fig. 2a, being the construction of another embodiment example of the authentication system using biometric system to which the present invention applies, shows a system allowing to perform an authentication procedure using biometric information in provision of various online services. Figs. 2b and 2c, being flow charts for another embodiment example of the authentication method using biometric information in accordance with the present invention, show authentication processes using the biometric information in the authentication system (using the biometric information) illustrated in Fig. 2a. Further, Fig. 2d, being the construction of an embodiment example of the database to which the present invention applies, shows a construction of a database for administering information relating to divisional storage of the biometric information.

As illustrated in Fig. 2a, the authentication system using biometric information as per the present invention is also applicable to a system for authentication procedure required for utilizing various services provided online, such as on the Internet. In other words, the biometric information, e.g. fingerprint information, voice information, iris information, etc. required for an authentication procedure for utilization of various online services, can be stored as divided in a plurality of storage means so that the divided biometric information stored in the plural storage means is combined to be used for an authentication procedure, or an authentication is performed separately for each of the

divided and separately stored biometric information, to allow an access to the service provided.

For the convenience of explanation, the process of dividing and separate storing of the divided biometric information is described below with example of fingerprint information among divergent biometric information. For instance, a user can store his fingerprint information divided in a plurality of different storage means of a biometric information administration system 20 and in a user terminal 11 for storage of the biometric information. Alternatively, the biometric information can be stored divided in the above biometric information administration system 20, in the user terminal 11 for storage of the biometric information in use by the user, and in an application services providing system 30. However, the storage means for the fingerprint information is neither limited to the above biometric information administration system 20, nor to the user terminal 11 for storage of the biometric information, nor to the application services providing system 30, but rather, any storage means or systems (biometric information storage systems) 40 that can store the fingerprint information and allow to utilize the stored fingerprint information when necessary, can be used.

At the first step of divisional storing of fingerprint information, a user generates his fingerprint information by directly accessing a biometric information administration system 20 and requesting a divisional storage of the biometric information required for a user authentication, or by accessing a biometric information system 20 through joining an application services providing system (e.g. an electronic commerce system or an online finance system) 30 which provides electronic commerce services and inputting his fingerprint information in accordance with the instructions of the biometric information administration system 20. Here, the user inputs his fingerprint using a user terminal 10 that

allows to input a user fingerprint and to connect to a network (202), and then, the inputted fingerprint information is transmitted to the biometric information administration system 20 (204). The above biometric information administration system 20 may be a portal authentication institution, or an authentication system in the application services providing system 30 that provides electronic commerce services or online financing services.

The biometric information administration system 20 divides the transmitted fingerprint information and stores each of the divided fingerprint information in different storage means 30, 40 in the biometric information administration system 20 or outside thereof, or transmits parts of the divided fingerprint information to user terminals 11 for storing biometric information selected by a user (206). In other words, the biometric information administration system 20 divides the fingerprint information transmitted and stores each of the divided fingerprint information in different plural storage means, or transmits the same to a storage means on a network designated by the user, e.g. to a user terminal 11 for storing biometric information such as the user's PC, or to an application service providing system 30, to store the same there.

Here, the biometric information administration system 20 stores information on the plural storage means containing the divided fingerprint information in a database together with the user information (208). As shown in Fig. 2d, a user code or a device code (MAC code, product serial number, etc) which the user has accessed is generated, and then, is stored and administered together with the fragment index of the divided fingerprint information (biometric information), storage means, access code for each storage means (IP/ID/PW, etc.), as well as other user information.

A user accesses various application service providing systems 30 and undergoes an authentication procedure in a state that his fingerprint information is stored through the

above process dividedly in a biometric information administration system 20 which is a portal authentication institution, in biometric information administration system in each of the various application service providing system 30, in a user terminal 11 for storing biometric information or a biometric information administration system 20 which the user uses personally, in a biometric information storage system 40 which the user has designated, and the like.

In other words, a user having accessed a desired application service providing system 30 using various user terminals 10 (210), inputs his fingerprint through a user terminal 12 for inputting biometric information, upon request by the application service providing system 30 for inputting his fingerprint, for a user authentication procedure (212).

A computer keyboard, a mouse, etc. having a fingerprint input window affixed thereto can be used as a user terminal 12 for inputting biometric information. Alternatively, various wired/wireless terminals such as PCS, PDA, electronic key and the like equipped with a fingerprint input window, can be used for this purpose as well.

Here, the application service providing system 30 transmits the user information (ID, PW, etc.) together with the inputted fingerprint information to the biometric information administration system 20, whereupon the biometric information administration system searches information on the storage means in which the user's fingerprint information is dividedly stored, using the user information (214).

After that, the biometric information administration system 20 performs an authentication procedure to determine whether or not a user is an authorized user, by connecting the fingerprint information stored dividedly in various storage means and comparing the same with the inputted fingerprint information (216). Here, a comparison can be made, by fetching the fingerprint information stored dividedly in various storage

means, and then, combining the same before the combined fingerprint information is finally compared with the inputted user fingerprint information. Alternatively, the user fingerprint information inputted for the purpose of user authentication can first be transmitted to each storage means so that a partial comparison of the inputted user fingerprint information with the divided fingerprint information of the user stored in each storage means is conducted by an internal system of the storage means storing the divided biometric information, to finally enable the biometric information administration system 20 to perform a user authentication based on the results of the partial comparisons by the internal system of each storage means. In other words, the system of each storage means dividedly storing the fingerprint information receives the fingerprint information inputted for the purpose of user authentication and compares the part of the fingerprint stored in its own storage means with the corresponding part of the received fingerprint information, and transmits the result of the comparison to the higher system, i.e. to the biometric information administration system 20, whereupon, the biometric information administration system 20 determines whether to authenticate the user at the end, based on the results transmitted.

Still another alternative would be, to compare each of the fingerprint information dividedly stored in various storage means with the fingerprint information to be authenticated, i.e. after having fetched each fingerprint information dividedly stored in various storage means, to make partial comparisons of each of this divided fingerprint information with the fingerprint information to be authenticated, in order to determine whether or not all the corresponding parts coincide with one another.

Since the process of utilizing a service after the authentication (218) is the same as that in a conventional online service providing system, a description thereof is omitted.

Although division of the fingerprint information and distribution of the divided fingerprint information are performed by a biometric information administration system 20 as in the above description of Fig. 2b, a user terminal 10 in personal use of a user can also divide the fingerprint information and transmit the divided fingerprint information to the storage means 20, 30, 40 as shown in Fig. 2c.

When the biometric information administration system 20 or the application service providing system 30 requests for fingerprint information, the user inputs his fingerprint via a user terminal 10 such as a PC that allows to input a fingerprint (252), whereupon the user terminal 10 divides the inputted fingerprint (254), and stores a part of the divided fingerprint information in a user terminal for storage of the biometric information the user chooses 11 (including a storage space in the above user terminal itself) (256), while the remaining divided fingerprint information as well as information on the above storage means are transmitted to the biometric information administration system 20 or to the application service providing system 30 (258).

Then, the biometric information administration system 20 or the application service providing system 30 stores the fingerprint information as transmitted, or having divided the same anew (260) in each storage means, while storing information on the storage means received from the user terminal 10 and information on the storage means in which each of them has stored, using a format as illustrated in Fig. 2d (262).

The above procedure of dividing and distributing the fingerprint information by the user terminal 10 aims to prevent transmission of undivided fingerprint information of a user to the biometric information administration system 20 via a network. To elaborate, since fingerprint information of a user inputted via a user terminal 10 is divided by the biometric information administration system 20 after the transmission in the method of Fig.

2b, there arises a problem that a residue of the user fingerprint information can exist in the network or the fingerprint information can be hacked, while the method of Fig. 2c allows to enhance the security, because the fingerprint information undergoes here a dividing process at the user terminal 10 and then, only the divided partial fingerprint information is transmitted to the biometric information administration system 20.

As described above, the above biometric information administration system 20 can be a portal fingerprint recognition system, and the above application service providing system 30 can be a biometric information administration system operating such a system of its own, or one operated in association with a biometric information administration system 20 which is the above fingerprint recognition system. Since the procedure after registration of the fingerprint information (264 to 268) is the same as that of Fig. 1b, a description thereof is omitted.

Next, a detailed description of the process of dividing the biometric information follows below.

In case the biometric information is fingerprint information, it can be divided as follows:

First, fingerprint information can be divided by its coordinate information, i.e. a fingerprint is divided into a plurality of parts taking its central point (the most curved point of the ridges that rise like a mountain range in a fingerprint) as the base coordinate, and then the fingerprint information of each divided area is extracted. For example, a fingerprint can be evenly divided into four (or other number) parts taking the central point as the base coordinate and the fingerprint information is stored as per the parts.

Second, fingerprint information can be divided by its minutiae. Since a fingerprint comprises a plurality of minutiae such as ending points (where a ridge ends after a soft

flow), bifurcation (where a ridge branches after a soft flow), and so on, fingerprint information can be divided through storing such information on ending points, bifurcations, etc., separately.

Third, fingerprint information can be divided by dividing the bit information of the fingerprint information in accordance with a predetermined rule. Since fingerprint information can be expressed by bit and byte information (one byte equals to eight bits) represented in 0 or 1, such bit and byte can be divided in accordance with a certain rule, and then stored separately. For example, information with one byte volume consisting of eight bits can be divided into two parts by dividing the even numbered bits from the odd numbered, and then the divided information can be stored separately; or the information can be divided into four parts by grouping two successive bits together, starting from the first bit, and then the divided pairs of bits can be stored separately.

Now, a description of the division of voice information follows.

Voice information can also be divided in various manners: e.g. it can be divided by frames with predetermined time intervals, by characteristics of frequencies, by bit or byte based on a predetermined rule, by characteristics comparable to the minutiae of fingerprint information, etc.

Further, iris information can also be divided by coordinate information, by characteristics, by bit information of the iris information, etc. like in division of the fingerprint information. Various methods for dividing biometric information are applicable to other biometric information in conformity with the characteristics of individual biometric information.

While the present invention has been described above with reference to the preferred embodiments and the related drawings, the scope of the rights of the present

invention is not limited thereto, but rather shall be determined by the claims attached herein below and their equivalents, allowing various alterations, modifications, and adjustments, not departing the spirit and the scope of this invention, as those skilled in the art will understand.

Industrial Applicability

As described above, the present invention allows division of biometric information suitable for use as an authentication means into a plurality of groups and storing of the divided biometric information separately in a plurality of storage means, instead of simply storing such biometric information in a single specific storage means, thus, it can enhance the security in a service providing system, because it can effectively bar an unauthorized user from acquiring a full authentication, even when a part of the biometric information has been stolen.

What is claimed is:

1. A method for authentication using biometric information, comprising:

a first step, wherein biometric information of a user to be registered is inputted from a biometric information input device,

a second step, wherein said biometric information is divided into a predetermined number of groups,

a third step, wherein said divided biometric information is stored separately in a plurality of storage means,

a fourth step, wherein biometric information of a user to be authenticated is inputted from a biometric information input device,

a fifth step, wherein said biometric information of said user to be authenticated inputted at said fourth step is divided in the same manner and same number of groups as in said second step, and

a sixth step, wherein said biometric information of said user to be authenticated as divided at said fifth step is compared with said divided (corresponding) biometric information stored in said plurality of storage means, and said user to be authenticated is authenticated to be an authorized user, if all (of said corresponding) information coincide.

2. The authentication method using biometric information as set forth in Claim 1, wherein said plural storage means are scattered at different places and are connected to via a communication network to a biometric information input device.

3. The authentication method using biometric information as set forth in Claim 2,

wherein the said sixth step comprises:

step 6-1a, wherein said divided biometric information of said user to be authenticated is received at said scattered plural places,

step 6-2a, wherein said divided biometric information of said user to be authenticated is compared with the corresponding divided biometric information stored in said scattered plural places, and

step 6-3a, wherein said user to be authenticated is authenticated to be an authorized user, if the comparisons at said step 6-2a yield that all corresponding information coincide.

4. The authentication method using biometric information as set forth in Claim 3, comprising an additional step of deleting said divided biometric information of said user to be authenticated at said scattered plural places after completion of said comparison.

5. The authentication method using biometric information as set forth in Claim 2, wherein the said sixth step comprises:

step 6-1b, wherein said divided biometric information stored in said scattered plural places is received via a communication network,

step 6-2b, wherein said divided biometric information as received at said step 6-1b is compared with the corresponding divided biometric information of said user to be authenticated, and

step 6-3b, wherein said user to be authenticated is authenticated to be an authorized user, if each of said divided biometric information received coincides with the corresponding divided biometric information of said user to be authenticated.

6. The authentication method using biometric information as set forth in Claim 5, comprising an additional step of deleting said divided biometric information received after completion of said comparison.

7. The authentication method using biometric information as set forth in Claim 1, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each divided fingerprint image.

8. The authentication method using biometric information as set forth in Claim 1, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

9. The authentication method using biometric information as set forth in Claim 1, wherein said biometric information is fingerprint information and said division is performed through division by bits of the fingerprint minutiae data extracted from a fingerprint.

10. A method for authentication using biometric information, comprising:

a first step, wherein biometric information of a user to be registered is inputted from a biometric information input device,

a second step, wherein said biometric information is divided into a predetermined number of groups,

a third step, wherein said divided biometric information is stored separately in a plurality of storage means,

a fourth step, wherein biometric information of a user to be authenticated is inputted from a biometric information input device,

a fifth step, wherein said divided biometric information stored separately in said plural storage means is connected to one another and is reconstructed to the original biometric information, and

a sixth step, wherein said reconstructed biometric information is compared with the biometric information of said user to be authenticated, and said user to be authenticated is authenticated to be an authorized user, if the biometric information coincides.

11. The authentication method using biometric information as set forth in Claim 10, wherein said plural storage means are scattered at different places and are connected to a biometric information input device via a communication network.

12. The authentication method using biometric information as set forth in Claim 1, wherein said fifth step comprises:

step 5-1, wherein said divided biometric information stored scattered in said plural storage means is transmitted to said communication network, and

step 5-2, wherein said divided biometric information thus received is connected too one another and reconstructed to the original biometric information.

13. The authentication method using biometric information as set forth in Claim 12 comprising an additional step of deleting said divided biometric information received

from said plural scattered places after completion of said connection.

14. The authentication method using biometric information as set forth in Claim 10, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each divided fingerprint image.

15. The authentication method using biometric information as set forth in Claim 10, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

16. An authentication method using biometric information, adopting a biometric information input device and an authentication device capable of performing user authentication based on the biometric information inputted through the biometric information input device, comprising:

a first step, wherein said biometric information input device receives biometric information of a user to be registered and divides the same into a predetermined number of groups,

a second step, wherein said biometric information input device stores a part of said divided biometric information and the user information identifying the respective biometric information, and transmits the other biometric information, said user information, and information on the biometric information input device itself to said authentication device,

a third step, wherein said authentication device stores said biometric information, said user information, and said information on said input device,

a fourth step, wherein biometric information of a user to be authenticated is inputted from said biometric information input device, and then divided in the same manner and same number of groups as in said first step,

a fifth step of confirming whether any biometric information stored in said biometric information input device at said second step coincides with said biometric information divided at said fourth step,

a sixth step of transmitting the coinciding biometric information together with the user information and the device information stored to the authentication device, if it has been confirmed at said fifth step that any coinciding biometric information exists,

a seventh step, wherein said authentication device searches biometric information corresponding to said user information and apparatus information received from said biometric information input device, and then transmits the same to said biometric information input device,

an eighth step, wherein said biometric information input device compares said biometric information received with said biometric information divided at said fourth step, and then transmits the results of comparison to said authentication device, if any coinciding biometric information exists, and

a ninth step, wherein said authentication device, upon receiving the results of said comparison reporting that coinciding biometric information exists, authenticates said user to be an authorized user.

17. The authentication method using biometric information as set forth in Claim 16, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each

divided fingerprint image.

18. The authentication method using biometric information as set forth in Claim 16, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

19. The authentication method using biometric information as set forth in Claim 16, wherein said biometric information is fingerprint information and said division is performed through division by bits of the fingerprint minutiae data extracted from a fingerprint.

20. The authentication method using biometric information as set forth in Claim 16, comprising an additional step of deleting said biometric information received from said authentication device by said biometric information input device after said ninth step.

21. The authentication method using biometric information as set forth in any one of Claims 16 through 20, wherein said biometric information input device is a fingerprint recognition key, said authentication device is a door lock, and the door lock is unlocked when said user is authenticated at said ninth step to be an authorized user.

22. An authentication method using biometric information, adopting a biometric information input device and an authentication device capable of performing user authentication based on the biometric information inputted through the biometric information input device, comprising:

a first step, wherein said biometric information input device receives biometric information of a user to be registered and divides the same into a predetermined number of groups,

a second step, wherein said biometric information input device stores a part of said divided biometric information and the user information identifying the respective biometric information, and transmits the other biometric information, said user information, and information on the biometric information input device itself to said authentication device,

a third step, wherein said authentication device stores said biometric information, said user information, and said information on said input device,

a fourth step, wherein information on a user to be authenticated is selected among user information stored in said biometric information input device,

a fifth step, wherein said biometric information input device receives information on the user to be authenticated inputted and divides the same in the same manner and number of groups as in said first step,

a sixth step of transmitting said user information selected at said fourth step and the device information to the authentication device, if it has been confirmed that said divided biometric information of said user to be authenticated coincides with said biometric information of said selected user stored in said biometric information input device,

a seventh step, wherein said authentication device searches the biometric information corresponding to said user information and said device information received from said biometric information input device, and transmits the same to said biometric information input device,

an eighth step, wherein said biometric information input device compares said

biometric information received with the biometric information divided at said fourth step, and transmits the results of said comparison to said authentication device, if the biometric information coincides, and

a ninth step, wherein said authentication device, upon receiving the results of said comparison reporting that coinciding biometric information exists, authenticates said user to be an authorized user.

23. The authentication method using biometric information as set forth in Claim 22, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each divided fingerprint image.

24. The authentication method using biometric information as set forth in Claim 22, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

25. The authentication method using biometric information as set forth in Claim 22, wherein said biometric information is fingerprint information and said division is performed through division by bits of the fingerprint minutiae data extracted from a fingerprint.

26. The authentication method using biometric information as set forth in Claim 22, comprising an additional step of deleting said biometric information received from said authentication device by said biometric information input device after said eighth step.

27. The authentication method using biometric information as set forth in any one of Claims 22 through 26, wherein said biometric information input device is a fingerprint recognition key, said authentication device is a door lock, and the door lock is unlocked when said user is authenticated at said ninth step to be an authorized user.

28. An authentication method using biometric information, adopting a biometric information input device and an authentication device capable of performing user authentication based on the biometric information inputted through the biometric information input device, comprising:

a first step, wherein said biometric information input device receives biometric information of a user to be registered and divides the same into a predetermined number of groups,

a second step, wherein said biometric information input device stores a part of said divided biometric information and the user information identifying the respective biometric information, and transmits the other biometric information, said user information, and information on the biometric information input device itself to said authentication device,

a third step, wherein said authentication device stores said biometric information, said user information, and said information on said input device,

a fourth step, wherein information on a user to be authenticated is selected among user information stored in said biometric information input device,

a fifth step, wherein said biometric information input device receives information on the user to be authenticated inputted and divides the same in the same manner and number of groups as in said first step,

a sixth step of transmitting said user information selected at said fourth step and the device information to the authentication device, if it has been confirmed that said divided biometric information of said user to be authenticated coincides with said biometric information of said selected user stored in said biometric information input device,

a seventh step, wherein said authentication device searches the biometric information corresponding to said user information and said device information received from said biometric information input device, compares the corresponding biometric information with the received biometric information of the user to be authenticated, and authenticates said user to be an authorized user, if the biometric information coincides.

29. The authentication method using biometric information as set forth in Claim 28, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each divided fingerprint image.

30. The authentication method using biometric information as set forth in Claim 28, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

31. The authentication method using biometric information as set forth in Claim 28, wherein said biometric information is fingerprint information and said division is performed through division by bits of the fingerprint minutiae data extracted from a fingerprint.

32. The authentication method using biometric information as set forth in Claim 28, comprising an additional step of deleting said biometric information received from said authentication device by said biometric information input device after said seventh step.

33. The authentication method using biometric information as set forth in any one of Claims 28 through 32, wherein said biometric information input device is a fingerprint recognition key, said authentication device is a door lock, and the door lock is unlocked when said user is authenticated at said seventh step to be an authorized user.

34. An authentication method using biometric information, adopting a biometric information input device and an authentication device capable of performing user authentication based on the biometric information inputted through the biometric information input device, comprising:

a first step, wherein said biometric information input device receives biometric information of a user to be registered and divides the same into a predetermined number of groups,

a second step, wherein said biometric information input device stores a part of said divided biometric information and the user information identifying the respective biometric information, and transmits the other biometric information, said user information, and information on the biometric information input device itself to said authentication device,

a third step, wherein said authentication device stores said biometric information, said user information, and said information on said input device,

a fourth step, wherein information on a user to be authenticated is selected among

user information stored in said biometric information input device,

a fifth step, wherein said biometric information input device receives information on the user to be authenticated inputted and stores,

a sixth step of transmitting said user information selected and the device information to the authentication device,

a seventh step, wherein said authentication device searches the biometric information corresponding to said user information and said device information received from said biometric information input device, and transmits the corresponding information to said biometric information input device,

an eighth step, wherein said biometric information input device connects said received biometric information to said biometric information stored at said second step, reconstructing the original biometric information, compares the same with said biometric information of said user to be authenticated, and transmits the results of said comparison to said authentication device, if the biometric information coincides, and

a ninth step, wherein said authentication device, upon receiving the results of said comparison reporting that coinciding biometric information exists, authenticates said user to be an authorized user.

35. The authentication method using biometric information as set forth in Claim 34, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each divided fingerprint image.

36. The authentication method using biometric information as set forth in Claim

34, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

37. The authentication method using biometric information as set forth in Claim 34, wherein said biometric information is fingerprint information and said division is performed through division by bits of the fingerprint minutiae data extracted from a fingerprint.

38. The authentication method using biometric information as set forth in Claim 34, comprising an additional step of deleting said biometric information received from said authentication device by said biometric information input device after said eighth step.

39. The authentication method using biometric information as set forth in any one of Claims 34 through 38, wherein said biometric information input device is a fingerprint recognition key, said authentication device is a door lock, and the door lock is unlocked when said user is authenticated at said ninth step to be an authorized user.

40. An authentication method using biometric information, adopting a biometric information input device and an authentication device capable of performing user authentication based on the biometric information inputted through the biometric information input device, comprising:

a first step, wherein said biometric information input device receives biometric information of a user to be registered and divides the same into a predetermined number of groups,

a second step, wherein said biometric information input device stores a part of said divided biometric information and the user information identifying the respective biometric information, and transmits the other biometric information, said user information, and information on the biometric information input device itself to said authentication device,

a third step, wherein said authentication device stores said biometric information, said user information, and said information on said input device,

a fourth step, wherein information on a user to be authenticated is selected among user information stored in said biometric information input device,

a fifth step, wherein said biometric information input device receives information on the user to be authenticated inputted and stores the same,

a sixth step of transmitting said biometric information stored at said second step, said biometric information of said user to be authenticated, said user information selected, and said device information to the authentication device, and

a seventh step, wherein said authentication device connects the biometric information corresponding to said user information received to said biometric information received from said biometric information input device that was stored at said second step, reconstructing the original biometric information, compares the same with said biometric information of said user to be authenticated, and authenticates said user to be an authorized user, if the biometric information coincides.

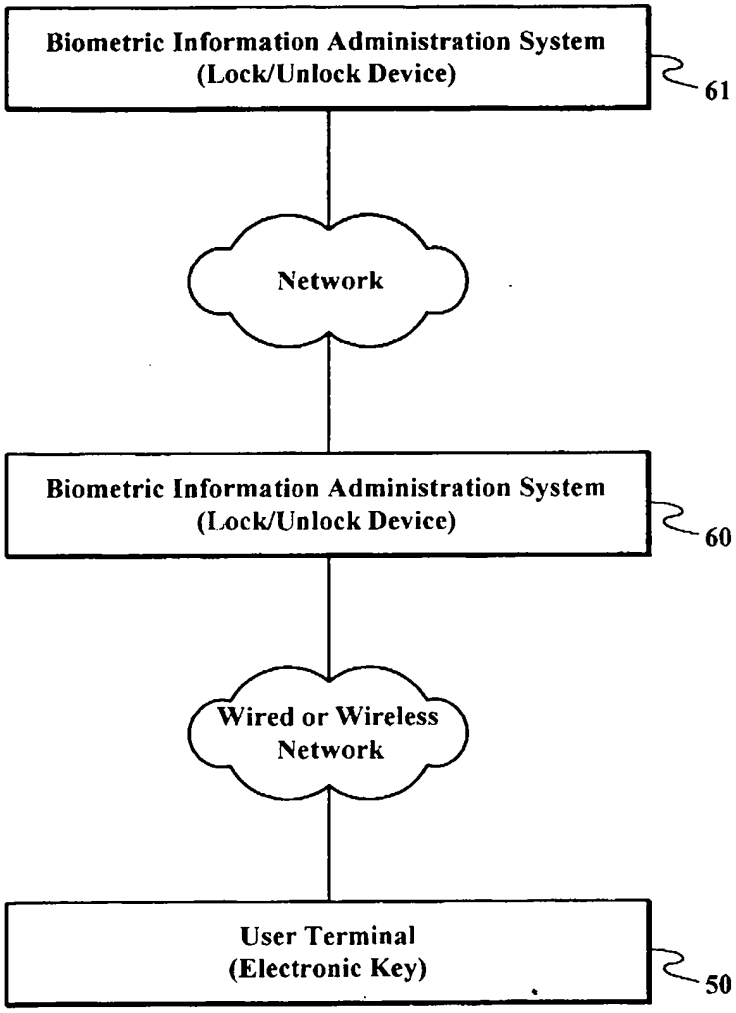
41. The authentication method using biometric information as set forth in Claim 40, wherein said biometric information is fingerprint information and said division is performed through spatial division of a fingerprint image and extracting minutiae of each divided fingerprint image.

42. The authentication method using biometric information as set forth in Claim 40, wherein said biometric information is fingerprint information and said division is performed through division of the minutiae obtained from an entire fingerprint image.

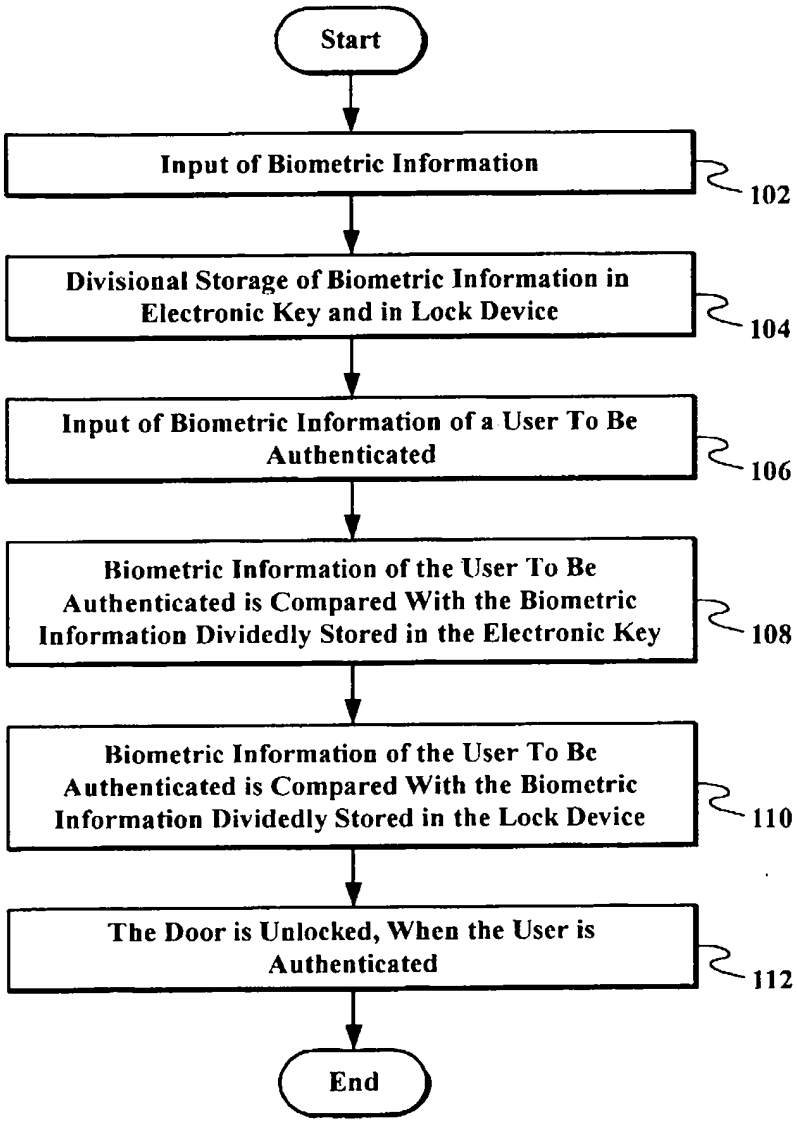
43. The authentication method using biometric information as set forth in Claim 40, comprising an additional step of deleting said biometric information received from said biometric information input device by said authentication device after said seventh step.

44. The authentication method using biometric information as set forth in any one of Claims 40 through 43, wherein said biometric information input device is a fingerprint recognition key, said authentication device is a door lock, and the door lock is unlocked when said user is authenticated at said seventh step to be an authorized user.

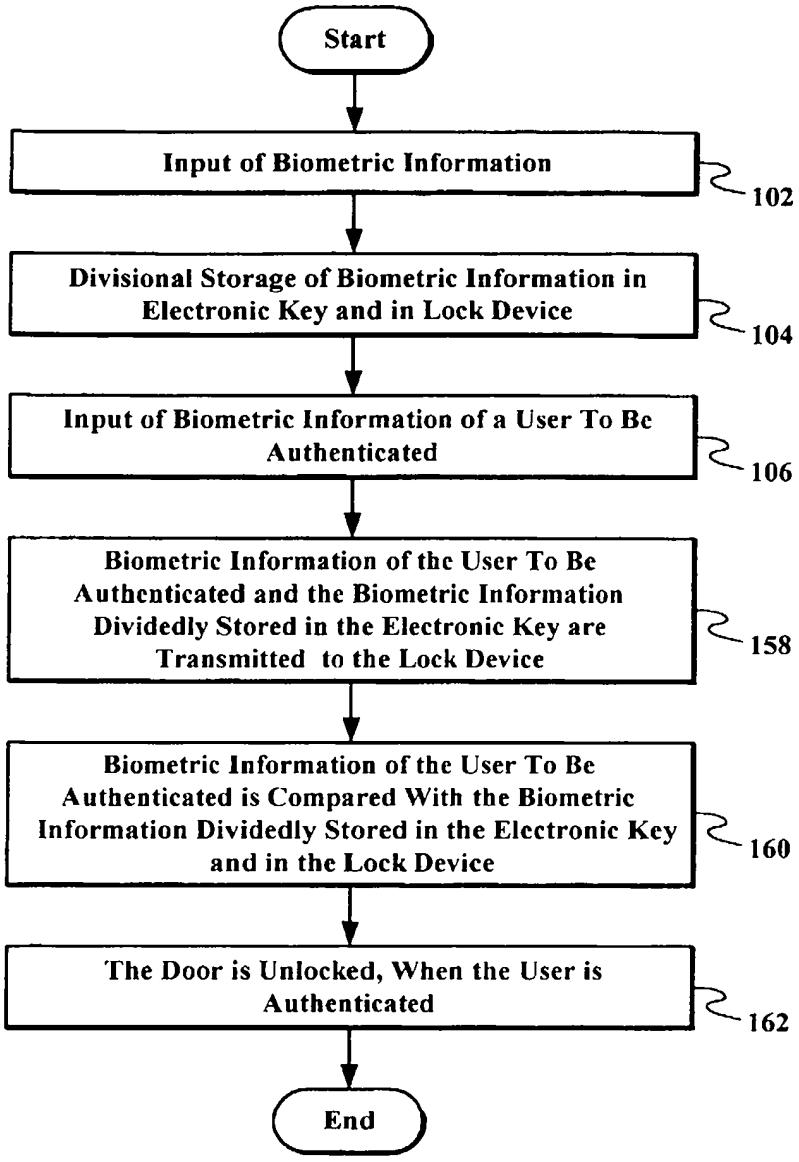
【Fig. 1a】


Biometric Information Administration System
(Lock/Unlock Device)
61
Network
Biometric Information Administration System
(Lock/Unlock Device)
60
Wired or Wireless
Network
User Terminal
(Electronic Key)
50

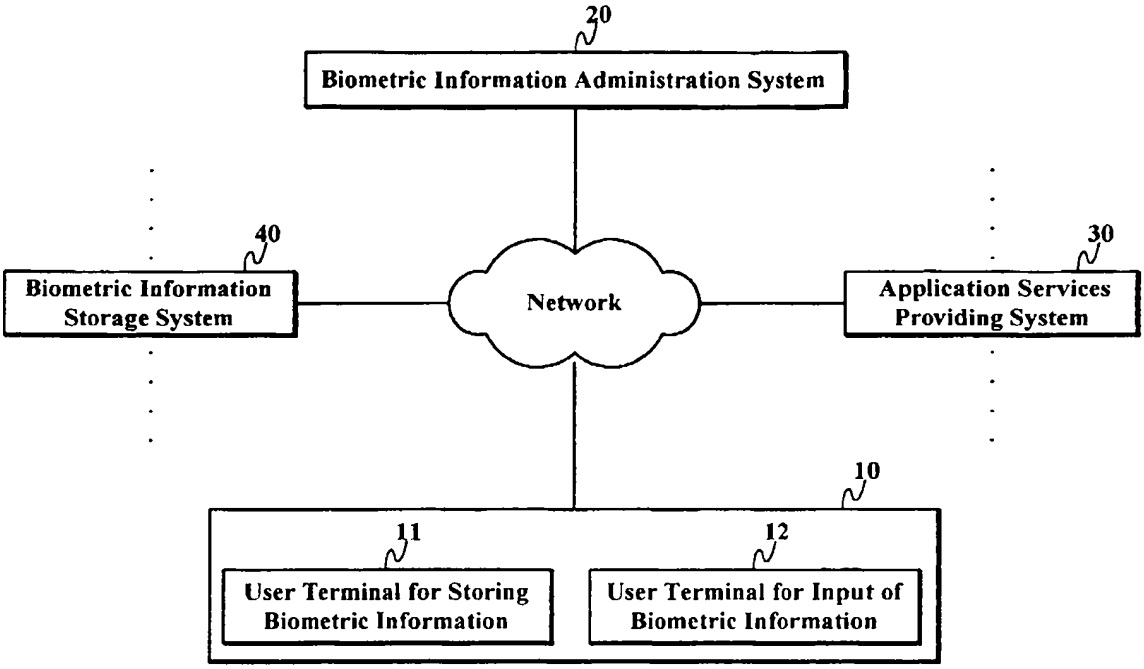
【Fig. 1b】


Start
Input of Biometric Information
102
Divisional Storage of Biometric Information in Electronic Key and in Lock Device
104
Input of Biometric Information of a User To Be Authenticated
106
Biometric Information of the User To Be Authenticated is Compared With the Biometric Information Dividedly Stored in the Electronic Key
108
Biometric Information of the User To Be Authenticated is Compared With the Biometric Information Dividedly Stored in the Lock Device
110
The Door is Unlocked, When the User is Authenticated
112
End

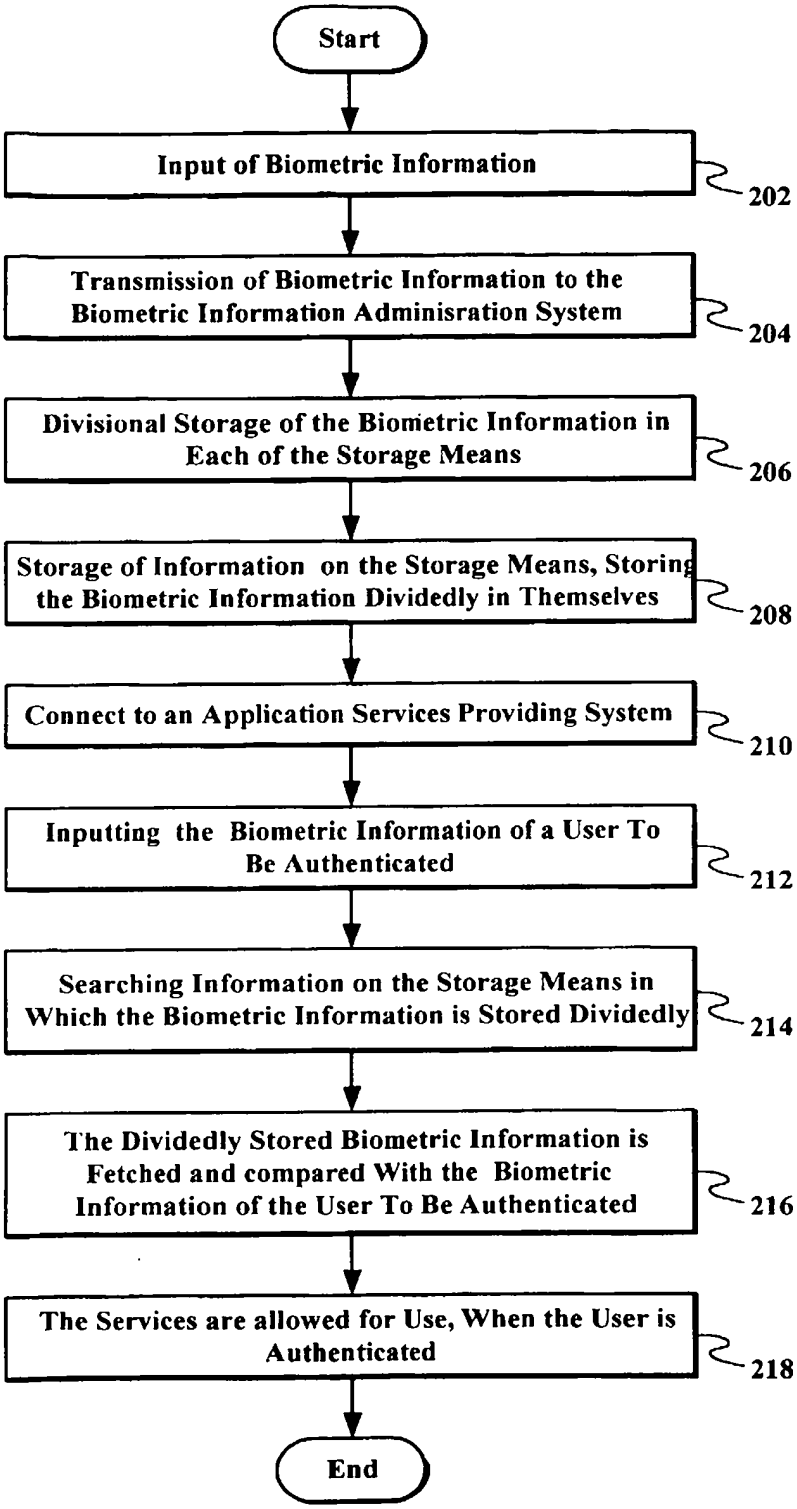
【Fig. 1c】


Start
Input of Biometric Information
102
Divisional Storage of Biometric Information in Electronic Key and in Lock Device
104
Input of Biometric Information of a User To Be Authenticated
106
Biometric Information of the User To Be Authenticated and the Biometric Information Dividedly Stored in the Electronic Key are Transmitted to the Lock Device
158
Biometric Information of the User To Be Authenticated is Compared With the Biometric Information Dividedly Stored in the Electronic Key and in the Lock Device
160
The Door is Unlocked, When the User is Authenticated
162
End

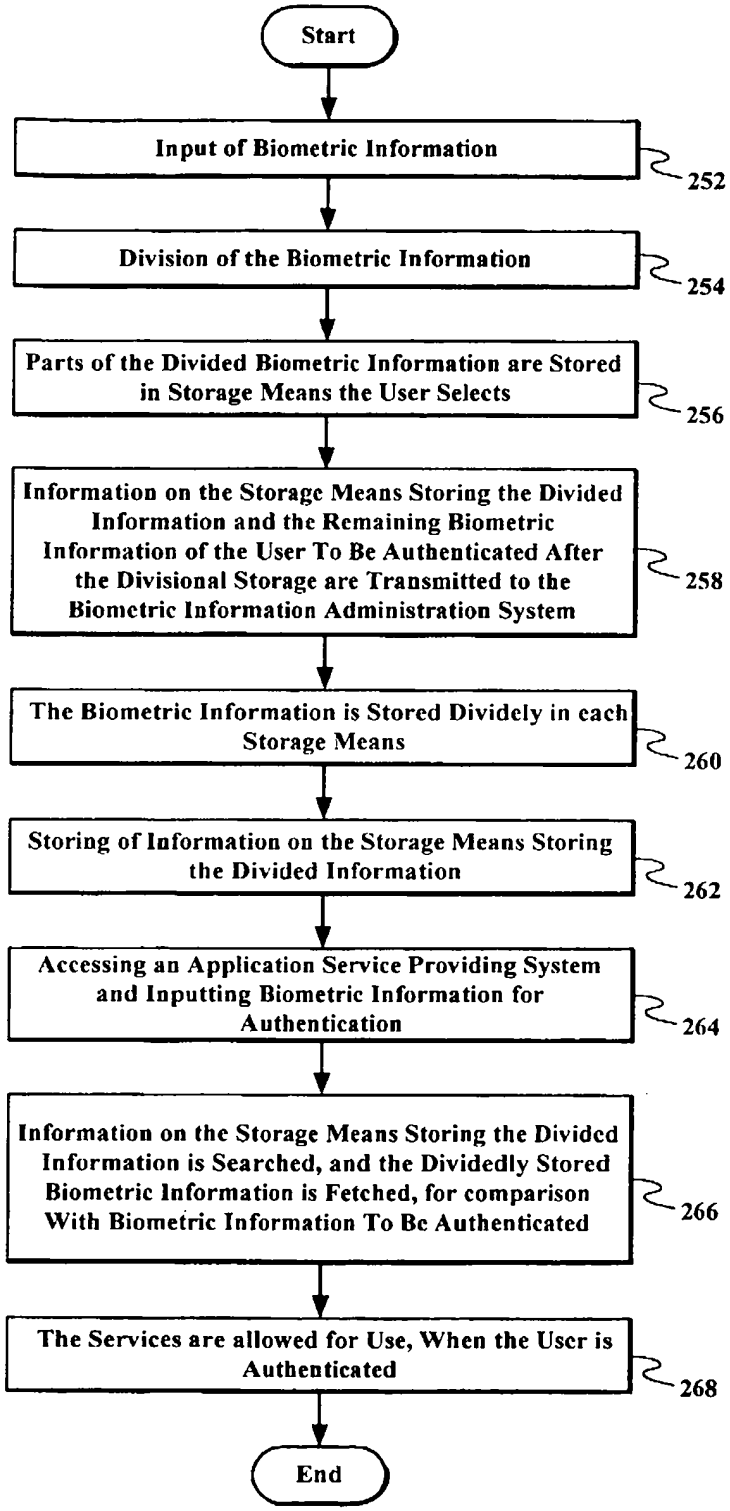
【Fig. 2a】


20
Biometric Information Administration System
40
Biometric Information Storage System
Network
30
Application Services Providing System
10
11
User Terminal for Storing Biometric Information
12
User Terminal for Input of Biometric Information

【Fig. 2b】


Start
Input of Biometric Information
202
Transmission of Biometric Information to the Biometric Information Adminisration System
204
Divisional Storage of the Biometric Information in Each of the Storage Means
206
Storage of Information on the Storage Means, Storing the Biometric Information Dividedly in Themselves
208
Connect to an Application Services Providing System
210
Inputting the Biometric Information of a User To Be Authenticated
212
Searching Information on the Storage Means in Which the Biometric Information is Stored Dividedly
214
The Dividedly Stored Biometric Information is Fetched and compared With the Biometric Information of the User To Be Authenticated
216
The Services are allowed for Use, When the User is Authenticated
218
End

【Fig. 2c】


Start
Input of Biometric Information
252
Division of the Biometric Information
254
Parts of the Divided Biometric Information are Stored in Storage Means the User Selects
256
Information on the Storage Means Storing the Divided Information and the Remaining Biometric Information of the User To Be Authenticated After the Divisional Storage are Transmitted to the Biometric Information Administration System
258
The Biometric Information is Stored Dividely in each Storage Means
260
Storing of Information on the Storage Means Storing the Divided Information
262
Accessing an Application Service Providing System and Inputting Biometric Information for Authentication
264
Information on the Storage Means Storing the Divided Information is Searched, and the Dividedly Stored Biometric Information is Fetched, for comparison With Biometric Information To Be Authenticated
266
The Services are allowed for Use, When the User is Authenticated
268
End

【Fig. 2d】

User Code No. or Device Code No.	Serial Number of the Partial Biometric Information	Storage Means	Access Passwords, etc	Other Information
01-XXXXX	01	Main Storage Means	IP, ID, PW	User Information, Device Code No., Personal Record, etc.
	02	Storage Means of (Publicly) Authorized Institutions	. . .	. . .
	03	Storage Means in User Homepages	. . .	. . .
	03	. . .	. . .	. . .

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR02/01251

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 G06K 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
(IPC7) G06K, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korea patents(utility models) and patent(utility model) applications for invention since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
KIPONET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP63145528A (OMRON TATEISI Electronics CO.) 17 June 1988 See the abstract and figures	1-43
A	JP05108805A (NIPPONDENSO CO. Ltd.) 30 April 1993 See the abstract	1-43
A	KR1992-0005022A (YOZAN Inc) 28 March 1992 See the abstract and figures	1-43
A	WO9926373A (Digital Persona Inc) 27 May 1999 See the abstract	1-43

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 NOVEMBER 2002 (13.11.2002)	13 NOVEMBER 2002 (13.11.2002)

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
920 Dunsan-dong, Seo-gu, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
JEON, Il Yong
Telephone No. 82-42-481-5981

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR02/01251

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR1992-0005022A	28.03.1992	US5239590A1 EP470530B1	24.08.1993 22.01.1997
WO9926373A	27.05.1999	US 1025676A EP1025676A1	19.09.2000 09.08.2000
JP63145528A	17.06.1988	NONE	
JP05108805A	30.04.1993	NONE	